

Appl. No. 10/002,882
Amdt. Dated November 1, 2005
Request for RCE

APP 1316

Remarks/Arguments

In the Final Rejection claims 23-39 were rejected, 35 USC 102(e), for the first time as anticipated by Giloi et al patent 6,850,985 (hereinafter Giloi). In response thereto applicants propose to cancel claims 24, 25, 30, and 35-39, to amend claim 28 to include the subject matter of its prior parent claim 23, to amend claims 26, 27, 31, and 33 to change the claim from which each individually depends, to amend claims 29, 31, and 32 to improve their form, and claim to amend claim 33 to include the subject matter of prior dependent claim 34.

Giloi and applicants are both directed to obtaining secure conferencing. But their concerns are directed to different problems involved with secure conferencing. Giloi's disclosure is directed to setting up secure conferences of diverse technologies or architectures. In particular, Giloi teaches how to combine existing industry standards, H.323 and TG.120, to establish secure multimedia conferences in IP networks. By allowing the use of network components, Gatekeepers and Gateways, Giloi also discloses how to establish conferences that span both IP and non-IP networks. Giloi's teaching is to obtain security by authentication of the parties involved in the conference and specifically by using two keys, namely, a public key and a private key; this is set forth beginning at column 8, line 62 of Giloi.

Giloi's teaching is therefore that a secure conference is obtained by authenticating the users/hosts (i.e., computers) who wish to participate in the conference. Giloi teaches the use of a digital certificate for authentication purposes. Giloi does acknowledge the possibility of encrypting the communication itself, but suggests that speed is more important for audio and video communications (see column 6, lines 33-44). At best, Giloi just alludes to the possible use of encryption of the communication itself, as at column 14, lines 42-50, "Some embodiments allow for establishing secure connections so that data is encrypted." and, at column 15, lines 33-35, "Furthermore, in other embodiments, the TCP connections may be advantageously restricted to transmitting secure encrypted data...". There is, however, absolutely no disclosure or teaching of any encryption/decryption for the communication itself as is actually necessary to achieve a high performance both with respect to security guarantees for the overall security of the conference communications and to solving problems of communication latencies incurred on conference data traffic. Needless to say, the problems of protecting distributed multimedia, multi-user conferences without imposing undue delays in the communications are not trivial.

Applicants' invention, which draws on technologies involving cryptography, distributed systems, communications protocols, and software engineering, solves these problems. Applicants' invention thus realizes secure, multimedia conferences in a distributed environment spanning both IP networks and non-IP networks (e.g., PSTN and Wireless). Specifically the security is attained not only by authentication of potential conference participants, but also by protecting the conference communication data by their novel and inventive cryptographic method. As described in applicants'

Appl. No. 10/002,882
Amdt. Dated November 1, 2005
Request for RCE

APP 1316

specification, a conference architecture (or a topology) realizes the secure multimedia conferences by delegating to individual conference processes (in a given conference) the responsibility for encrypting/decrypting communication payloads and mixing incoming streams of communication payloads. Different conferences have different conference keys.

Applicants' invention can thus be viewed as directly the opposite of Giloi's teaching. Whereas Giloi teaches a specific procedure for authenticating the user on the conference (utilizing known properties of industry standards H.323 and T. 129) but assumes that you can use any known encryption techniques for securing the communication itself, if you want to, applicants suggest the use of known authentication techniques ("In an illustrative embodiment, the security processor 274 executes the Kerberos security protocol for user authentication and key generation", page 5, lines 19-21) but employ specific novel and inventive procedures for securing the communication.

Claim 28, which has been amended to be an independent claim, specifically recites, in accordance with this aspect of applicants' invention, that the step of securing the communication is distinct from the step of authenticating the user who wants to participate in the conference and further involves the use of a secret conference session key and protecting the secret session key with a second secret key. Claim 29, dependent on claim 28, further recites steps involved in the step of securing the communication including decrypting the message data using the secret conference session key prior to the client process mixing the communications from a plurality of conference participants.

In rejecting claims 28 and 29 the Examiner has merely repeated applicants' actual claim language and then referred to Giloi column 8, line 30 to column 10, line 30. Applicants have reviewed these paragraphs which, as discussed above, relate to authenticating the conference participant using a public key and a private key. None of this is relevant to the recitations in claims 28 and 29 of applicants' invention concerning the provision of security of the communication itself and not the authentication of the conference participants, as discussed above.

The Examiner, in rejecting prior independent claim 23, also asserted that Giloi involves mixing communications from a plurality of participants. However, the recitation, now appearing in amended claim 28, is that a client process associated with the user mix the communications from a plurality of conference participants. Applicants submit that this aspect of applicants' invention is neither disclosed nor suggested by Giloi.

The Examiner had rejected dependent claim 27 again by quoting applicants' claim language and then citing Giloi Fig. 4, column 10, lines 31-46, and column 12, lines 20-30. Fig. 4, which is described at column 10, depicts a single conference. Giloi at column 12 discusses that a conference participant can quit a conference. None of this is relevant to applicants' recitation in dependent claim 27 of the aspect of applicants' invention involving further functions of the client process, namely that a client process enables a user to participate simultaneously in more than one conference and to proactively notify

Appl. No. 10/002,882
Amdt. Dated November 1, 2005
Request for RCE

APP 1316

other users of any changes to these conferences. Applicants have described the creation of new conferences from existing conferences in the section entitled Conference Spawning at page 17, lines 11-30 of their specification.

Claim 31 and its dependent claim 32 also recite that aspect of applicants' invention wherein a user is participating simultaneously in more than one conference and specifically in one conference involving one type of media device and in a second conference involving a different type of media device. In rejecting claim 31 the Examiner had again cited Fig. 4, column 10, lines 31-46 but has added column 13, line 53-column 14, line 6. That latter material discusses the use of H.323 standards to enable a computer to communicate with a variety of targets. Then in rejecting claim 32, dependent on claim 31, the Examiner has cited column 1, line 63-column 2, line 10 and column 14, lines 52-64. The material at columns 1 and 2 discusses the differences between H.323 and T.120 standards, while the material at column 14 discusses isolating processing pertinent to one conference connection from another conference connection. Applicants again suggest that this is not relevant to the simultaneous multiple conference calls as recited in claims 31 and 32.

Applicants' claim 33, which now includes the subject matter of prior claim 34, is directed to an aspect of applicants' invention involving persistent conferences and the conference server retaining identification of participants who have left a persistent conference. While the material at column 14, line 52 to column 15, line 20 discusses adding participants to a conference, there is no disclosure or suggestion there or at column 7, lines 1-16 of applicants' invention involving persistent conferences as recited in claim 33.

Applicants respectfully submit that the claims as amended and as proposed herein present no new issues, and, accordingly, withdrawal of the Final Rejection and entrance of this Amendment are requested. Further applicants deem that, as discussed above, none of the claims being presented is anticipated by Giloi, that is, the claims do not read upon the disclosure of the Giloi patent nor are they obvious in view of the Giloi disclosure and teaching. Favorable consideration and allowance of claims 26-29, and 31-33, as amended, and passage of this application to issue are respectfully requested.

Appl. No. 10/002,882
Amdt. Dated November 1, 2005
Request for RCE

APP 1316

If the Examiner believes it would in any way expedite the prosecution of this application and avoid the necessity of an appeal, the Examiner is invited to telephone applicants' attorney at the number set forth below.

Respectfully submitted,

Chit Chung et al

By 

James W. Falk
Attorney for Applicants
Reg. No. 16,154
(732) 699-4465